INITIAL STUDIES ON WORM PROPAGATION IN MANETS FOR FUTURE ARMY COMBAT SYSTEMS

Robert G. Cole
JHU Applied Physics Laboratory
Laurel, MD, 20723 *

31 September 2004

ABSTRACT

This study presents an analysis of computer worm propagation in a Mobile Ad-hoc Network (MANET). According to the recent DARPA BAA - *Defense Against Cyber Attacks on MANETS* (DARPA, 2004), "One of the most severe cyber threats is expected to be worms with arbitrary payload that can infect and saturate MANET-based networks on the order of seconds". Critical to the design of effective worm counter measures in MANET environments is an understanding of the propagation mechanisms and their performance. MANET technologies are expected to play a key role in the Future Combat System (FCS). This work aims to advance the security of these critical systems through increasing knowledge of propagation mechanisms, performance and the effect of future mitigation technologies. We present both analytic and simulation analysis of worm propagation. This study focuses on features of a tactical, battlefield MANET which are unique to this environment. The ultimate goal of these studies is to develop an accurate set of performance requirements on potential mitigation techniques of worm propagation for tactical, battlefield MANETS.

1. INTRODUCTION

There is much emphasis within the DARPA BAA on Digital Cyber-Attacks in MANETS(DARPA, 2004) on computer worm propagation, mitigation and isolation. For this reason we have performed an initial investigation of computer worm propagation in tactical, battlefield MANETS. The primary goal of this research effort is the generation of a set of performance requirements on potential mitigation technologies in order to ensure their success in tactical, battlefield MANETS. This objective drives some of the modeling parameters we choose to investigate in this study. This report contains our initial investigations and analysis of the performance of worm propagation and mitigation techniques. Special attention is paid to the impact of the communications characteristics found in tactical, battlefield MANETS and their impact on worm propagation. For example, a model which captures the self-throttling aspects of the competition between multiple instances of the same worm in accessing the limited bandwidth in a MANET is analyzed in the context of our simulation studies.

Over the past five to ten years, the Internet has experienced a number of computer worm attacks on its connected hosts. These worm attacks include the the Code Red I and II and Nimda Worms (Staniford et al., 2002), and others. Investigators have extensively studied the design of the worms' propagation mechanisms as well as their strategies for spreading (Staniford et al., 2002), (Moore and Shannon, 2003), (Moore et al., 2003), (Zou et al., 2002), (Wang and Wang, 2003), (Serazzi and Zanero, 2001). These mechanisms and strategies include various address space searching algorithms and methods to spread at rates below intrusion detection system thresholds.

The standard analytic model used in the literature to analyze worm propagation in computer networks is the Standard Epidemic Model (e.g., (Zou et al., 2002) and (Bailey, 1975)), i.e.,

$$\frac{dI(t)}{dt} = \beta I(t)[N - I(t)]/N \tag{1}$$

where N is the total size of the susceptible population, $I(t)$ is the number of infected nodes at time t, and β is the rate at which a given infected node probes the total, susceptible population of nodes.

Key assumptions in the derivation of the Standard Epidemic Model applied to worm propagation in computer networks are:

- *Action at a Distance* - as soon as an infected probe is queued for transmission to another host, it is immediately received by that host. This implies that all hosts always have routes established to

[*] R. Cole is with the Power Projection Department, JHU/Applied Physics Laboratory, Rm. 17-S476, 11000 Johns Hopkins Road., Laurel, Maryland. E-mail: robert.cole@jhuapl.edu

Report Documentation Page	*Form Approved* *OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **00 DEC 2004**	2. REPORT TYPE **N/A**	3. DATES COVERED **-**

4. TITLE AND SUBTITLE **Initial Studies On Worm Propagation In Manets For Future Army Combat Systems**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **JHU Applied Physics Laboratory Laurel, MD, 20723**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

See also ADM001736, Proceedings for the Army Science Conference (24th) Held on 29 November - 2 December 2005 in Orlando, Florida. , The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**UU**	**8**	

all other hosts and hence there exists no time required for the route discovery process. It also implies that there exists no queuing, transmission or propagation delays within typical, bandwidth constrained, tactical, battlefield MANETS. This effect can be significant in MANETS.

- *Independent Infection Agents* - there exists no interaction between the infection probes propagating through the infection media, i.e., the communication network. In networks, and prominently in MANETS, this ignores two effects, a) sharing access to a common communications facility such as the radio channel and b) probe losses due to overloading the limited bandwidth and finite sized communication buffers. These effects can also be quite large in MANETS as we discuss below.
- *Zero Death Rate* - once a node is infected it never dies or gets cured. Instead, it is forever infected and generating infection probe packets. This assumption is related to the modeling of mitigation mechanisms within the MANETS and to the determination of their effectiveness in protecting the majority of the nodes.
- *No Incubation Period* - as soon as the infection probe packet reaches the susceptible computer hosts, it can immediately begin transmitting infection probes to the other hosts. Generally, there may be some time required for the infection to incubate within the newly infected host, but we suspect this to be a small effect in most environments

Through modifications to the Standard Epidemic Model and through extensive simulation studies, we investigate each of these assumptions within the context of a tactical, battlefield MANET. Several of these assumptions have been addressed within other studies, e.g., bandwidth constrained propagation, but in different contexts than the one addressed here, i.e., fixed wired Internet-like environment. We analyze worm propagation across a range of MANET design parameters. We present simplified numerical models (compared to previous studies) which nonetheless capture relevant aspects of worm propagation and mitigation techniques. As such, we hope to discover explicit solutions to these simplified models which would prove useful in future engineering studies.

Our results demonstrate that the *Action at a Distance* and the *Independent Infection Agents* assumptions are clearly not valid in MANETS due to route discovery mechanisms and delays, nodal mobility, limited bandwidth and the multi-access radio channel. Therefore, models of worm propagation through MANETS must incorporate these effects. Our analysis concludes with a discussion of these results within the context of generating performance requirements on potential mitigation technologies.

2. PREVIOUS STUDIES

Previous studies have analyzed and modeled the propagation of computer worms in digital communications networks. (Staniford et al., 2002) provided an extensive investigation into the mechanisms of worm propagation and their performance, addressing specifically the Code Red I and II worms as well as the Nimda worm. They also provide an interesting discussion on potential strategies to build better worms and efforts necessary to mitigate worm propagation throughout the Internet. (Moore and Shannon, 2003) and (Moore et al., 2003) provided an investigation of the Code Red worms propagating through the Internet. Relevant to our work, they provide an interesting discussion and analysis of performance requirements on several mitigation technologies through simulation studies of Internet-like networks.

(Zou et al., 2002), provide an excellent analysis of mathematical models of worm propagation through the Internet. Notably, they discuss the Kermack-Mckendrick model for the removal of infected nodes from the system. They also propose a heuristic expression for inter-worm competition for Internet bandwidth and develop a “Two Factor Worm Model” for their studies. Finally, they provide a thorough review of mathematical models of epidemics and provide references.

(Wang and Wang, 2003) address the issues of finite propagation times and infected node removal (or death) on propagation rates. They provide both analytic models and simulation results of these effects for Internet-like environments. Finally, (Serazzi and Zanero, 2001), provide a thorough literature review of worm propagation models and studies. Interestingly, they also review various models of mitigation techniques of computer worm propagation.

3. ANALYTIC MODELS

In this section we discuss several analytical models of worm propagation in computer networks. We draw upon previous models, but derive simplified forms while maintaining their critical aspects. Our hope being to encourage simple, explicit solutions useful to engineers in future studies. We will rely upon the models discussed herein to analyze our simulation results of worm propagation through MANETS.

The Standard Epidemic Model is derived, based upon the set of assumptions discussed in Section 1, from the following difference equation,

$$I(t+\Delta t) \approx I(t)+\beta I(t)\Delta t[N-I(t)]/N+O((\Delta t)^2) \quad (2)$$

where $I(t)$ is the number of infected nodes at time t, β is the rate at which a given infected node probes the total, susceptible population of nodes, N, and $O((\Delta t)^2)$ represents terms of order $(\Delta t)^2$. Here, $\beta I(t)\Delta t$ is the effective number of probes which are sent into the target network and $[N - I(t)]/N$ represents the probability that a probe encounters a susceptible, non-infected node. The target network in our discussion is the set of nodes composing the MANET. In the limit that $\Delta t \to 0$, dividing through by Δt, we get

$$\frac{dI(t)}{dt} = \beta I(t)[N - I(t)]/N \quad (3)$$

Defining the probability of infection as $i(t) = I(t)/N$, we rewrite the equation as

$$\frac{di(t)}{dt} = \beta i(t)[1 - i(t)] \quad (4)$$

An explicit solution to the Epidemic Model, obtained by factoring and integration, is given by

$$i(t) = \frac{e^{\beta(t-T)}}{1 + e^{\beta(t-T)}} \quad (5)$$

where T is determined by the initial condition $i(t = 0)$.

Typically, β is written as

$$\beta = \beta_0(\frac{N}{2^{32}}) \quad (6)$$

where β_0 represents the rate at which an individual, infected node probes for other nodes and $N/2^{32}$ represents the likelihood that a randomly chosen 32-bit IPv4 address is a valid network node. Other strategies are employed and modeled accordingly through appropriate definitions of β. In our study, in order to concentrate on those aspects unique to MANET networks, we assume that the infection worms only generate probes to nodes within the MANET. In this case β will be set to the rate at which an individual infected node generates and transmits probes. This represents a worse case strategy from the perspective of generating performance requirements on mitigation techniques and assumes that the worms will have access to a table of nodes comprising the MANET. However, it is somewhat artificial in the sense that the infected nodes chooses from the table of nodes randomly. Clearly, additional node selection strategies should be the subject of future investigations.

Eq.(5) results in the viral spreading rate as shown in Figure 1. The results in this figure were generated for the Baseline parameter set given in Table 1. It is important to note (see the discussion below in Section 5), that this and other models to be presented, model the mean infection propagation for a given set of parameters and say nothing regarding the variation in the spreading rate.

The Kermack-Mckendrick model (Frauenthal, 1980) addresses the issue of the removal process of infected nodes. In the context of computer worm propagation, (Zou et al., 2002) applied the Kermack-Mckendrick model in their study of the Code Red worm. This extension to the Standard Epidemic model addresses the *Infinite Lifetime* assumption discussed above and is important in the context of our mitigation technology discussion below. We can derive a relatively simple numerical model of the performance of mitigation technologies as follows. Let $c(t)$ be the probability that a host has been infected by the worm by time t. This represents both the probability of hosts currently infected, $i(t)$, and the probability of hosts either quarantined or rehabilitated (and no longer susceptible to further infection), $r(t)$. Let us assume a simple model of the mitigation technology, i.e., that it takes a fixed amount of time (ζ) for the mitigation response to act on the infected hosts. Then, following the same argument to derive the Standard Epidemic model above, we get

$$\frac{dc(t)}{dt} = \beta(c(t) - c(t - \zeta))[1 - c(t)] \quad (7)$$

This relatively simple equation can be used to understand the mean behavior of the worm propagation when competing with a deployed mitigation technology. Note, this equation can also be derived from the more complex "Two Factor Worm Model" found in (Zou et al., 2002), by realizing that the term $c(t)-c(t-\zeta) = i(t)$ and that $c(t) = i(t)+r(t)$. This expression modifies the Standard Epidemic model above by arguing that the total probe rate within the network is modified by the removal of the nodes which had been infected prior to $t-\zeta$ seconds ago. This simple equation will be used later to get a sense of the effectiveness of mitigation or quarantine mechanisms in stopping the spread of infection through a network.

(Wang and Wang, 2003) have addressed the issue of propagation delays and their effects on worm propagation in wired network environments. Again, a simple extension of the Standard Epidemic model addressing the *Action at a Distance* assumption is obtained by replacing $\beta I(t)$ on the RHS of Eq.(1), with $\beta I(t - \delta)$ where the δ represents (here) the fixed propagation delay of the infection probe between the time it is produced and queued within the infection agent to the time it reaches and infects a new, susceptible node. Note that this substitution is also applicable in relaxing the assumption of *Zero Incubation Period.* Making this substitution in Eq.(1), we get

$$\frac{di(t)}{dt} = \beta i(t-\delta)[1-i(t)] \qquad (8)$$

For times on the order of δ, this modification will be reflected in the slower than standard initial spread of the worm throughout the network. For times much larger than δ, the predictions of this expression approach those of the Standard Epidemic model. Hence, this expression is useful in analyzing the initial growth dynamics found in our simulation studies.

Of primary interest in tactical, battlefield MANET environments is the limited bandwidth available to the mobile nodes and the contention mechanisms for access to the radio channel. As worms attempt to propagate through a MANET, these factors become important influences on the rate of propagation. As the infection grows, the various infected nodes begin competing for the scarce channel bandwidth. As the infection probability grows, the multi-access channel becomes a 'self-throttling' mechanism. This gets to the issue of the assumption of *Independent Infection Agents.*

Several studies have discussed these effects within the context of wired, fixed networks of the type and size of the Internet (Staniford et al., 2002), (Zou et al., 2002), (Serazzi and Zanero, 2001). (Zou et al., 2002) proposed a heuristic expression to capture this effect in Internet environments. Specifically, they proposed replacing β with a time dependent $\beta(t)$ as

$$\beta(t) = \beta_0[1-i(t)]^\eta \qquad (9)$$

where η is a scaling parameter, which in our studies is a function of the probe size, the radio channel bandwidth and the density of the nodes in the MANET. We wish to test this heuristic in the analysis of our simulation studies and to combine this expression with the model incorporating the finite propagation delay of the probes across the MANET. Doing so results in the following expression capturing these two effects,

$$\frac{di(t)}{dt} = \beta_0 i(t-\delta)[1-i(t-\epsilon)]^\eta[1-i(t)] \qquad (10)$$

where ϵ represents a time somewhere between 0 and δ. Remember that we are trying to model the effect of probe traffic on the overall congestion within the MANET. The question becomes (in this joint model) how to capture the fact that the congestion is increasing over the propagation time of a given probe. It would see a level of congestion somewhere between $[1-i(t-\delta)]^\eta$ and $[1-i(t)]^\eta$. One way to address this factor is to assume a midpoint in time, which the ϵ factor reflects. However, we will assume that the propagation time of a probe, i.e., δ, is small compared to the overall worm spreading time (which is validated by our simulation studies) and therefore set $\epsilon = 0$. Hence our joint equation becomes

$$\frac{di(t)}{dt} = \beta_0 i(t-\delta)[1-i(t)]^{\eta+1} \qquad (11)$$

It turns out that the above heuristic does a very good job of fitting the simulation data, although η is a free ranging parameter. It is of interest to determine if a model of the competition in a wireless MANET can be constructed, which reasonably fits the data and provides a more explicit interpretation of the model parameters. This will be investigated in future work.

4. SIMULATION STUDIES

The NS2 simulation tool (NS2, 2004) was used to simulate the spread of the worm infection throughout a MANET. The version 2.27 of NS2 already contained an application which simulated the spread of a computer worm. We modified the NS2 application in order to a) simulate an isolated MANET and b) allow us to plant the initial infection seed at random in the MANET at time zero.

Because the dynamics specific to a MANET are of interest, we simplified the simulation and analysis in the following ways:

- Simple Worm Model - we assume the worm propagates through the transmission of a single UDP packet of size P. We simulate the effects of bandwidth competition by varying the channel bandwidth while holding the size of the infection data constant.

- MANET Aware Model - the worm chooses nodes at random to infect, but only targets nodes within the MANET. We wanted to focus this initial study on MANET specific issues, without the added complexity of modeling and simulating on-MANET versus off-MANET probe traffic.

- Modified Random WayPoint Mobility Model - we assumed that the nodes moved independent of one another according to the Random WayPoint model, modified in order to address the concerns raised in (Yoon et al., 2003). Other, more realistic, mobility models will be studied in the future, e.g., see (Camp et al., 2002).

- AODV Routing Protocol - the NS2 simulation tool supports a number of MANET routing protocols. For our initial studies we choose the AODV routing protocol (Perkins and Royer, 2001). Future studies will include other routing protocols.

Table 1: Baseline Case parameter definitions.

Parameter Description	Range	Base Case
Number of Hosts	50	50
Address Block Search	50	50
Transmission Rate (Mbps)	0.1 - 2.0	2.0
Transmission Range (m)	250	250
Topographic Range (m^2)	1000^2	1000^2
Nodal Mobility (mps)	1 - 10	1
Routing Protocol	AODV	AODV
Probe Size (bytes)	400	400
Probe Rate (probes/sec)	1	1

- 802.11 MAC and Physical Layer - The NS2 simulation tool provides models of the 802.11 MAC and Physical layer protocols. Further, we utilized the NS2 Two Ray radio propagation model with an effective transmission range of 250 meters.

The parameters in Table 1 define our Baseline MANET simulation model.

Several simulations of the Baseline Case were conducted. These results allowed us to first assess the variability between simulation runs and to determine the appropriate number of simulation runs for each study. Based upon an analysis of the standard deviations in the separate runs, we choose to carry out 30 separate, independent runs for each study reported in this paper. These initial runs also allowed for the assessment of the fit of the Standard Epidemic Model on the simulated performance of worm propagation through MANETS. Figure 1 shows the average results from a set of 30 independent simulation runs of the Baseline parameter set defined in Table 1. Each point in the plot represents the average time at which the infection probability incremented by $1/N$. The line through the simulation points is simply a smoothed representation of the simulation runs. Also in Figure 1 we plot the numerical prediction of worm propagation from the Standard Epidemic model. We see that the Standard Epidemic model overestimates the propagation rate of the worm within the MANET.

The breakdown of the Standard Epidemic model in Figure 1 in predicting the short term behavior of the worm propagation is due to the *Action at a Distance* assumption. To study this effect (and the *Independent Infection Agent* assumption) further, we made a series of simulation runs in which we varied the channel bandwidth from a high of 2.0 Mbps down to a low of 100 Kbps. The results, from this set of runs, are shown in Figure 2. These results show that the channel bandwidth starts to become a limiting factor between 1.0 Mbps and 400 Kbps for the parameter set studied. This is reflected both in the short term behavior (harder to see in this plot) and the long term behavior. This slower worm propagation is good from the perspective of mitigation technologies, but of course means that the radio channel is congested. In Figure 3, we superimpose several numerical predictions from Eq.(8), from the simplified Wang and Wang model, over a subset of the bandwidth limiting simulation runs. This figure shows the numerical predictions for propagation delays ranging from 0 seconds up to 5 seconds. It appears from this figure that the best fit to the initial startup period is the finite propagation model with a delay of around 1.0 seconds. Running through a set of more detailed curve fitting for the various bandwidth simulation runs we find the best propagation delays for each bandwidth as given in Table 2. Figure 4 shows an example for the bandwidth of 200 Kbps. We see excellent fit of the numerical results to the simulation for the short term phase of the worm propagation due to the incorporation of the finite propagation delay from this figure.

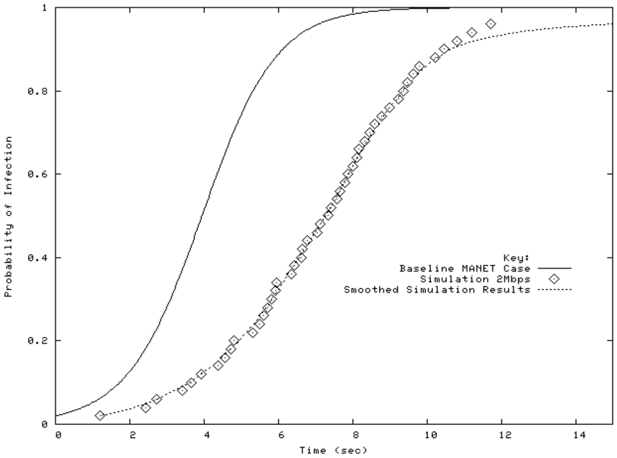

Figure 1: The baseline MANET worm propagation results.

Table 2: Fit of δ and η parameters to simulation data.

Bandwidth	δ	η
2000 Kbps	1.00	0.10
1000 Kbps	1.00	0.15
400 Kbps	1.05	1.50
300 Kbps	1.06	2.30
200 Kbps	1.20	4.00
100 Kbps	2.00	6.10

However, looking back at Figure 3, we see that the long term time behavior at lower bandwidths are not yet captured in the numerical predictions due to the competition for bandwidth between the numerous probes. Figure 5 shows an example result of curve fitting the heuristic competition model for lower bandwidth runs, i.e., 400 Kbps channels. Even in these high competition cases the heuristic model of (Zou et al.,

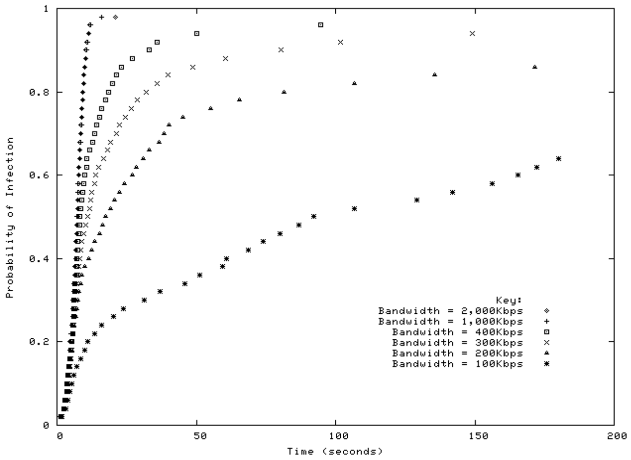

Figure 2: The effects of reduced channel bandwidth on worm propagation.

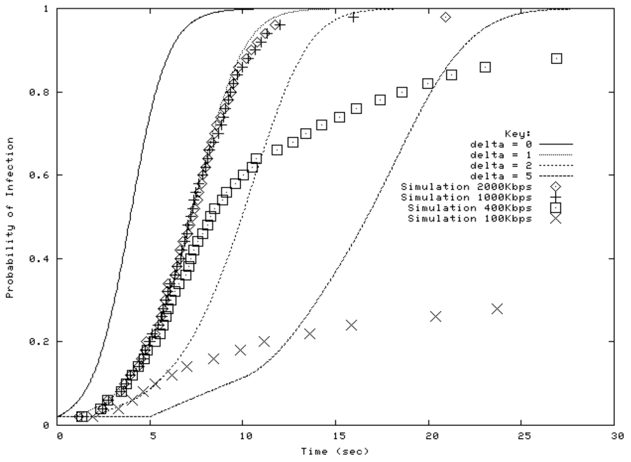

Figure 3: The predictions of the Wang and Wang model for various propagation delays.

2002) fits the simulation data well. Table 2 gives the values of η used for the various simulation runs versus channel bandwidth. As we expect, the value of η increases as the channel bandwidth decreases. For the lower bandwidths, i.e., 100 to 300 Kbps, we find that the η parameter is in the range of 2 to 6 demonstrating a high competition between the infection agents.

Finally, we ran a set of simulations to investigate the impact of node mobility on worm propagation rates. These results are shown in Figure 6. It appears that for the parameter set we are investigating, node mobility has little effect on the propagation of the worm. It was not clear at the outset, what these results would show. On one hand, higher mobility is expected to cause higher probe delays due to route changes. On the other hand, higher mobility could increase worm propagation due to breaking topologies where isolated islands may exist.

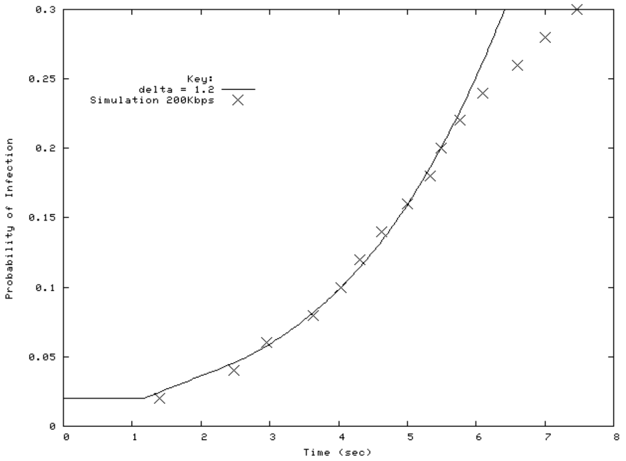

Figure 4: The *Action at a Distance* model fitting at high resolution for a 200 Kbps channel.

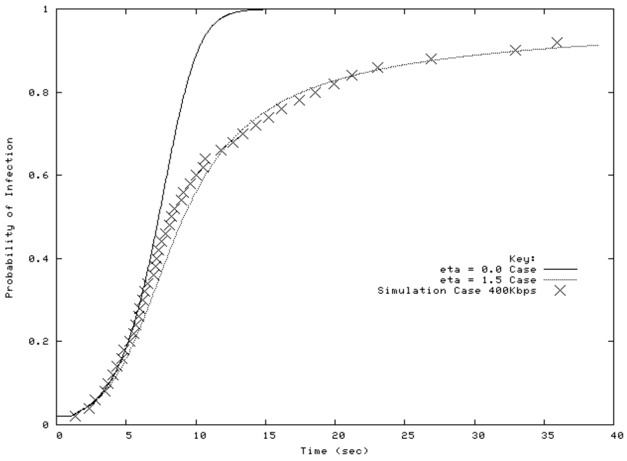

Figure 5: The heuristic model of probe competition at lower bandwidths, i.e., 400 Kbps.

The simulations run to date represent an initial set of studies on the propagation of computer worms. These studies focused on numerically modeling the impact of finite probe propagation delay and probe competition under various channel bandwidths and nodal mobilities. Other parameter impact studies are underway looking at various nodal densities, alternate routing protocols, etc. Of the studies reported in this paper, the numerical models of Section 3 predict the spread of computer worms within MANETS, although each of these models contain at least one fitting parameter. It is clearly desirable to develop from first principles explicit expressions for these fitting parameters and remove the dependence of a fitting parameter in our predictions. This is work for future studies.

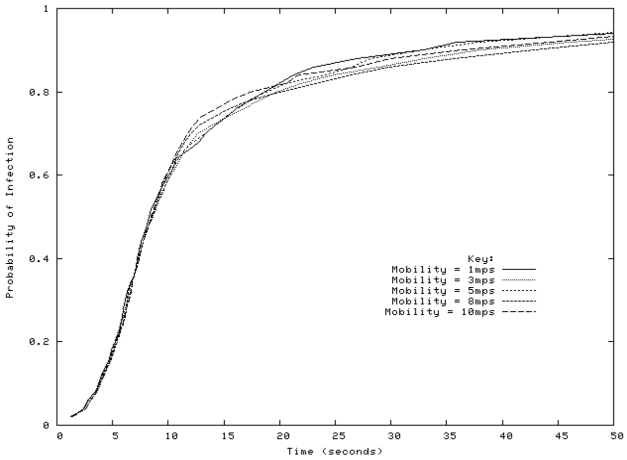

Figure 6: The effects of node mobility on worm propagation for the 400 Kbps case.

5. DISCUSSION OF MITIGATION TECHNOLOGIES

Modeling investigations presented thus far have focused on greedy worm propagation mechanisms whereby the worms propagate at a high rate, eventually stressing the underlying communication infrastructure. In these situations, it is reasonable to expect that intrusion detection monitoring systems would detect the worm propagation traffic patterns and could be used to initiate some form of response, e.g., nodal quarantines, nodal patches, etc. An alternative worm propagation strategy, as discussed in (Staniford et al., 2002), is a stealth strategy whereby the worm intentionally propagates at an extremely low rate; operating below an intrusion detection system (IDS) threshold. Once the network infection probability is high, then these stealth worms can reveal their existence and in some sense maximize their attack effectiveness. This latter strategy may be countered by integrity checking systems on the nodes comprising the MANETS. Therefore, it seems that an effective countermeasure may consist of IDS methods to disrupt greedy worm propagation working on a relatively fast time scale, in conjunction with integrity checking systems to catch the presence of worms propagating under a stealth strategy. But how fast would IDS and associated rehabilitation or quarantine measures have to be to keep the spread of the worm to acceptably low values in tactical, battlefield MANET environments?

Eq.(7) above presents a simple numerical model of mitigation technique effectiveness. Some results from this model are shown in Figure 7 for the model parameters defining our *Baseline Case* and for values of ζ ranging from a low of 4 seconds to a high of 12 seconds. We see that mitigation response times greater than 10 or so seconds have little affect on the mean behavior of the worm infection, while a response time of roughly 4 seconds reduces the mean infection probability to less than 0.3 in this example.

The above numerical model addresses only the mean behavior of the propagation. In order to derive meaningful requirements for mitigation technologies, we need to investigate the effectiveness of the mitigation technologies in keeping the worm infection probability below some value, say, 95 percent of the time. (Moore et al., 2003) studied this question in the context of the larger, wired Internet. They examined, through simulation of several potential mitigation technologies such as *Address Blacklisting* and *Content Filtering*, the spread of a computer virus through a large scale network. The focus of (Moore et al., 2003) was on the effectiveness of these mitigation technologies in reducing the worm infection versus the probing rate of the worm. They evaluated the effectiveness of these technologies in terms of various confidence levels.

Clearly this is the direction we need to take our studies in order to generate performance requirements on potential mitigation technologies. Figure 8 gives us an idea of the variability in the worm propagation in a typical MANETS by plotting out the individual histories from a set of 30 simulation runs. The parameters used for this set of runs were the *Baseline Case* with the exception that the channel bandwidth was set to 400 Kbps. The mean value numerical models may not satisfy our needs to generate useful requirements on mitigation technologies. However, it is interesting to note that the variability in the short time behavior is relatively small and it is over this time scale that IDS-like mitigation technologies must act in order to be effective. Our future investigations will require further simulation studies and perhaps the development of meaningful stochastic differential equations for worm propagation in computer networks.

6. CONCLUSIONS

We have presented an initial study of computer worm propagation in MANETS. We investigate the validity of these models through simulation studies of a worm propagation model. Our simulation studies address the effects of radio channel bandwidth and node mobility on propagation rates of the computer worm. These studies demonstrate that the effects of finite propagation delays and bandwidth competition can strongly influence the propagation rates of computer worms. The results of these studies agree with the predictions of the our simplified analytical models for these environments. Our ultimate goal is to generate performance requirements on potential mitigation

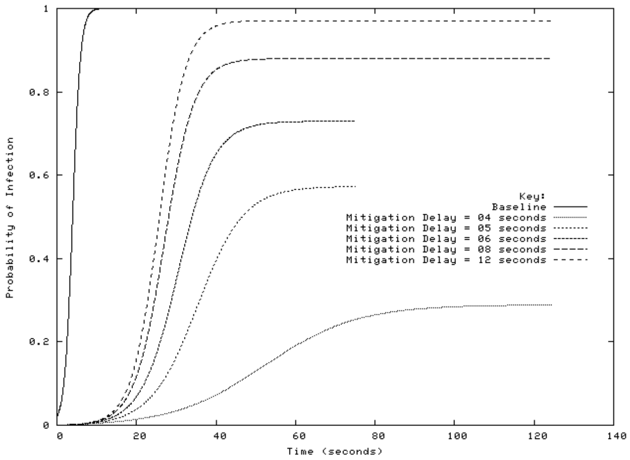

Figure 7: The baseline worm propagation with mitigation results.

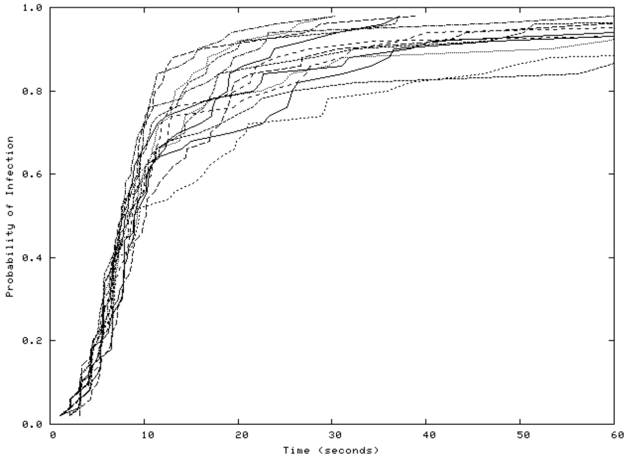

Figure 8: The variation in propagation rates for the worm propagation over 400Kbps radio channels.

technologies in these MANET environments. We concluded this report with a brief discussion of modeling the effectiveness of mitigation technologies and future investigations.

7. ACKNOWLEDGMENTS

I would like to acknowledge Sue Lee of JHU/APL for suggesting this investigation and for her initial encouragement, beneficial discussions and a host of references on the topic. Also, Amy Castner of JHU/APL provided information on the general nature of worm propagation and references. Finally, I wish to thank Nam Phamdo and Steve Jones of JHU/APL for their detailed review of the manuscript and excellent suggestions for future investigations in this area.

References

Bailey, N.T., *The Mathematical Theory of Infectious Diseases and it's Applications*, Hafner Press, New York, 1975.

Camp, T., Boleng, J. and V. Davies, *"A Survey of Mobility Models for Ad Hoc Network Research"*, Wireless Communication and Mobile Computing (WCMC), vol. 2, no. 5, 2002.

Ghosh, A.K., Technical POC, *Defense against Cyber Attacks on Mobile, Ad Hoc Network Systems (MANETS)*, BAA04-18 Proposer Information Pamphlet (PIP), Defense Advanced Research Projects Agency (DARPA) Advanced Technology Office (ATO), 16 April 2004.

Frauenthal, J.C., *Mathematical Modeling in Epidemiology*, Springer-Verlag, New York, 1980.

Moore, D. and C. Shannon, *"Code-Red: a Case Study on the Spread and Victims of an Internet Worm"*, in Proceedings of the 2002 SIGCOMM Internet Measurement Workshop, Marseille, France, pp. 273-284, November 2003.

Moore, D., et al., *"Internet Quarantine: Requirements for Containing Self-Propagating Code"*, in Proceedings of the 2003 SIGCOMM Internet Measurement Workshop, Marseille, France, pp. 273-284, November 2003.

The Network Simulator - 2, *http://www.isi.edu/nsnam/ns/*, 2004.

Perkins, C.E. and E.M. Royer, *"The Ad Hoc On-Demand Distance-Vector Protocol"*, in *Ad Hoc Networking*, C.E. Perkins (ed.), Addison-Wesley, 2001.

Serazzi, G. and S. Zanero, *"Computer Virus Propagation Models"*, preprint, 2001.

Staniford, S., Paxson, V. and N. Weaver, *"How to Own the Internet in Your Spare Time"*, in Proceedings of the 11th USENIX Security Symposium, 2002.

Wang, Y. and C. Wang, *"Modeling the Effects of Timing Parameters on Virus Propagation"*, in WORM'03, Washington D.C., October 2003.

Yoon, J., Liu, M. and B.D. Noble, *"Random Way Point Considered Harmful"*, in INFOCOM '03 (San Francisco), April 2003.

Zou, C.C., Gong, W. and D. Towsley, *"Code Red Worm Propagation Modeling and Analysis"*, in CCS'02, Washington, D.C., November 2002.